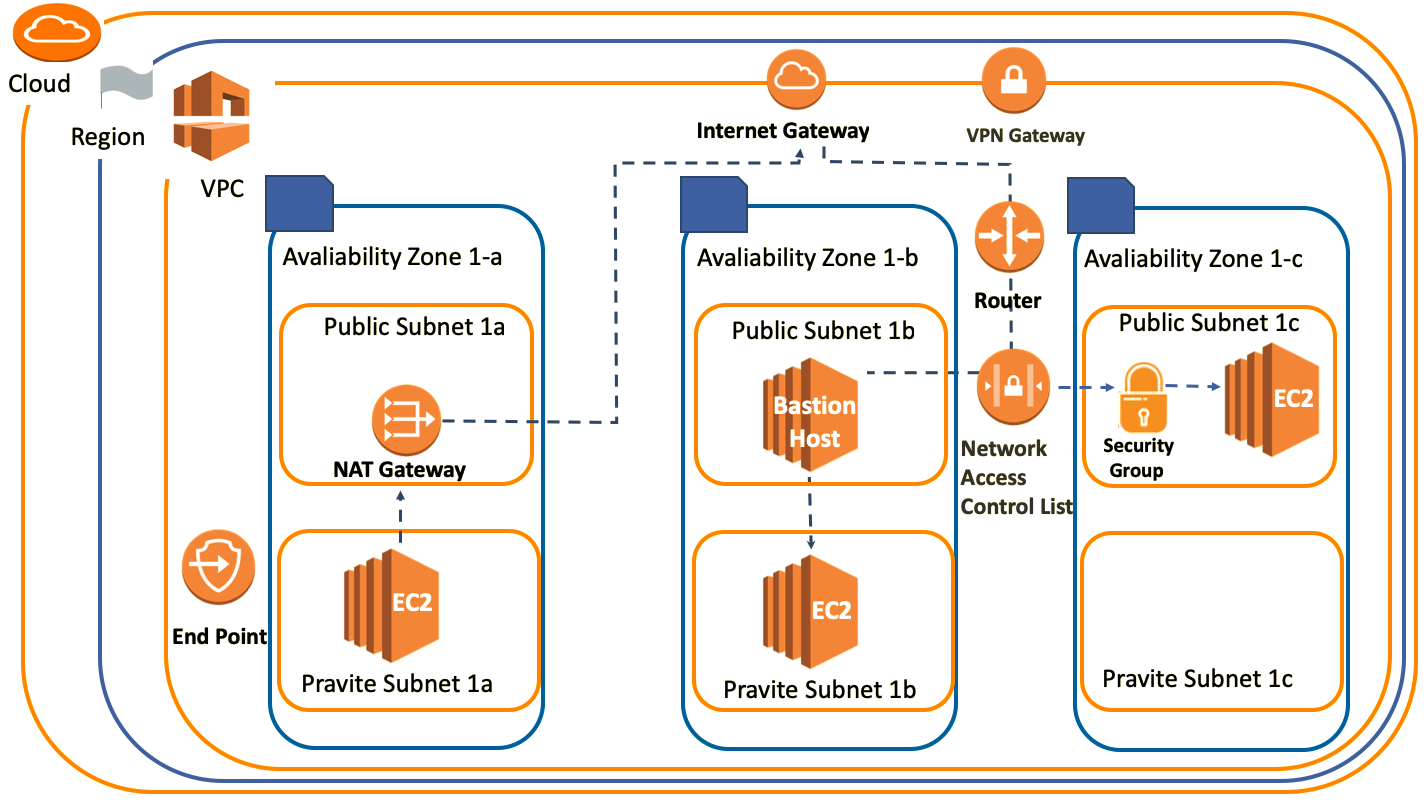
VPC

Anahtarlar, yönlendiriciler, tekrarlayıcılar, güvenlik duvarları, ağ kablolarıyla bağlanan yük dengeleyiciler gibi aygıtlar aracılığıyla oluşturduğumuz fiziksel ağların iletişim bölümünü sağlayabiliriz.

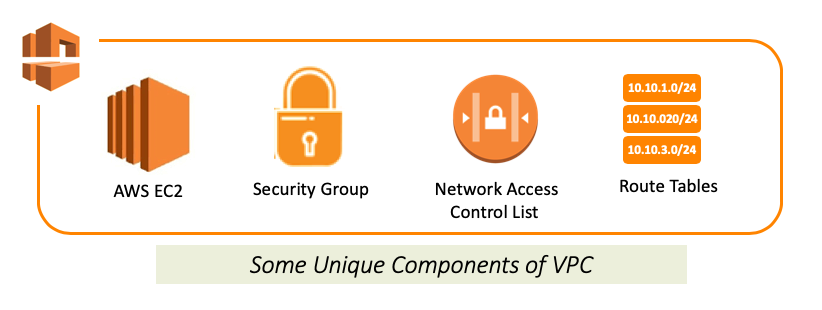
Ancak bulut söz konusu olduğunda, artık eriştiğimiz ve yapılandırdığımız fiziksel bir ağ yok. Bu fiziksel ağı simüle eden ve üzerinde mantıksal yapılar oluşturmamıza izin veren sanal yapılar var. AWS dünyasında buna VPC denir.

Kısacası, Amazon Sanal Özel Bulutu (Amazon VPC), AWS bulutunun tanımladığınız bir sanal ağda başlatabileceğiniz mantıksal olarak yalıtılmış bir alandır. Böylece VPC, AWS kaynaklarınız üzerinde çok daha iyi güvenlik kontrolü sağlar.



Yukarıda görülen resim VPC Mimarisini göstermektedir. Aşağıdaki derslerde, bu mimariye dayalı olarak VPC'nin nasıl oluşturulacağını ve bileşenlerinin çalışma yöntemini göreceğiz.

VPC structure



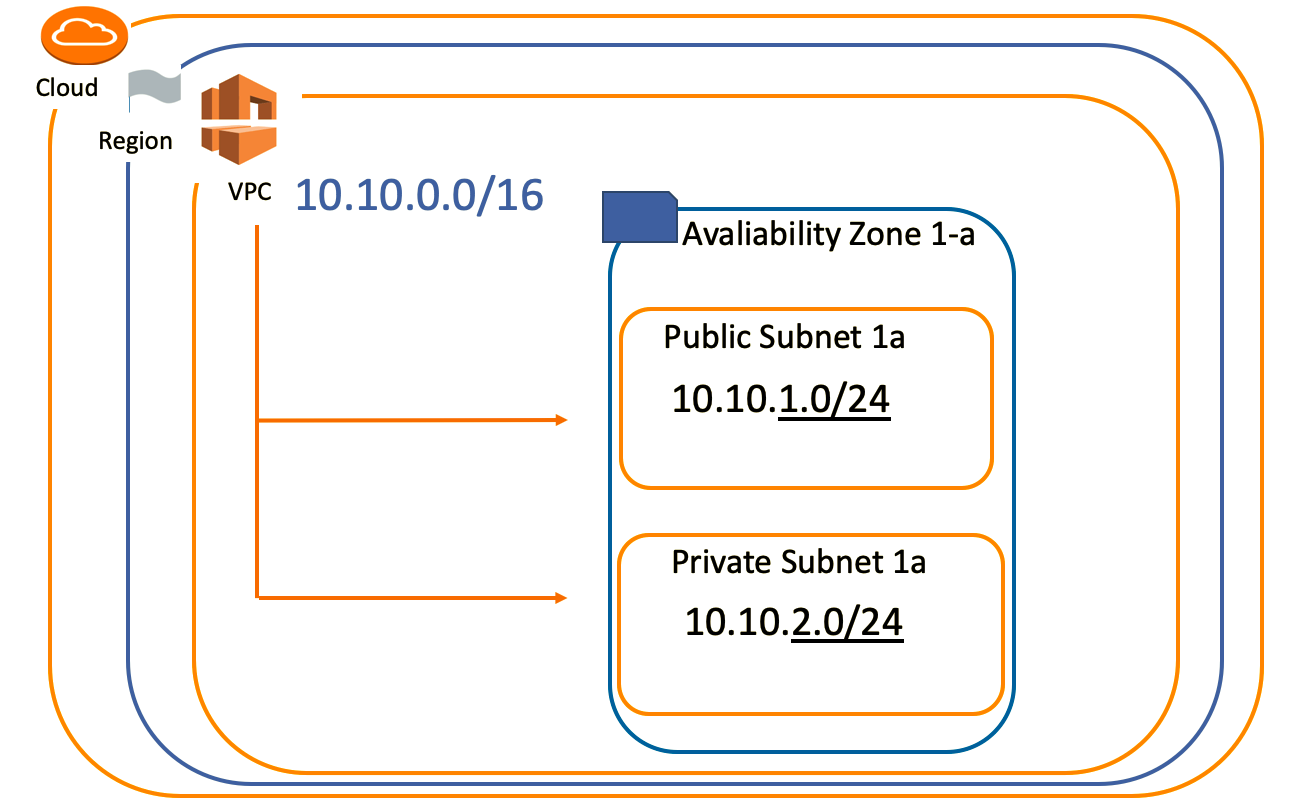
VPC, kendi özel ağ yapımızı oluşturabildiğimiz, kaynaklarımızı çalıştırabildiğimiz ve mantıksal olarak izole edebileceğimiz bir sanal ağ katmanıdır. Böylece VPC, kendi IP adres aralığınızı seçme, Subnetlar oluşturma, kök tabloları ve gateawaylerini yapılandırma da dahil olmak üzere sanal ağ ortamınız üzerinde tam denetime izin verir.

AWS, dünya genelinde veri merkezlerinin kümelendiği fiziksel bir yer olan bir Bölge kavramına sahiptir. Her AWS Bölgesi, AWS'ye Başlarken bölümünde hatırladığınız gibi bir coğrafi alanda birden çok, yalıtılmış ve fiziksel olarak ayrı AZ'den oluşur.

Her bölge; bir varsayılan VPC ile birlikte gelir ve her bölge için 5 VPC daha oluşturabiliriz. Bu 5'lik yumuşak bir sınırdır ve 5'ten fazla VPC'ye ihtiyacımız olursa AWS'den talep edebiliriz.

VPC'ler tek bir bölgeyle ilişkilidir. VPC'yi bölgelere dağıtamazsınız.

AWS şu anda dünyanın 22 coğrafi bölgesinde 70 Kullanılabilirlik Bölgesi'ni kapsamakta ve Endonezya, İtalya, Japonya, Güney Afrika ve İspanya'da on altı tane daha Kullanılabilirlik Bölgesi ve beş AWS Bölgesi daha planladığını açıklamıştır.



Subnet, VPC'nizdeki bir dizi IP adresidir.

VPC'de tanımladığımız ana IP bloğunu, Subnet adı verilen alt mantıksal ağlara böleriz. Bu şekilde, aynı özelliklere sahip bileşenleri kolayca kümeleyebiliriz.

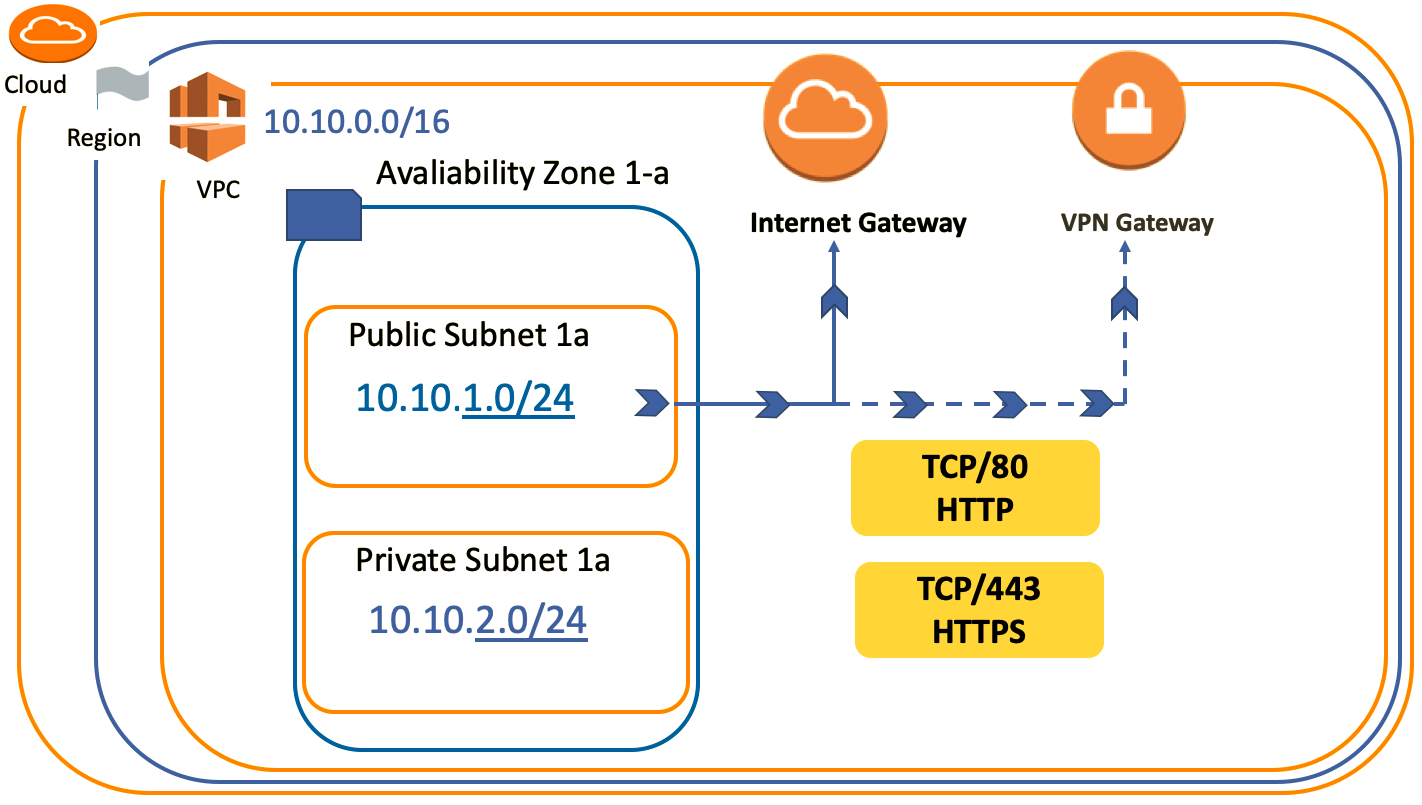
Subnetlar 2 tip olabilir: Genel Subnet ve Public Subnet.

Genel Subnet dediğimizde, Subnetlara yerleştirdiğimiz sanal makinelere VPC'nin dışından erişilebilir (Genel internet).

Özel olarak adlandırılan Subnetlara yerleştirdiğimiz makineler yalnızca VPC aracılığıyla iletişim kurma olanağına sahiptir. Bu şekilde, kaynaklarımızı yetkisiz erişime karşı korur ve ağ güvenliği sağlıyoruz.

Ayrıca, her Subnet yalnızca belirli bir AZ'de (Kullanılabilirlik Bölgesi) oluşturulabilir. Bir Subnet birden fazla AZ ile ilişkilendirilemez.

Internet Gateway&VPN Gateway



Diyelim ki VPC ve Subnetlarımızı oluşturduk. Ancak internete bağlanmalarını nasıl sağlayabiliriz? Cevap Internet Gateway veya VPN Gateway'dir.

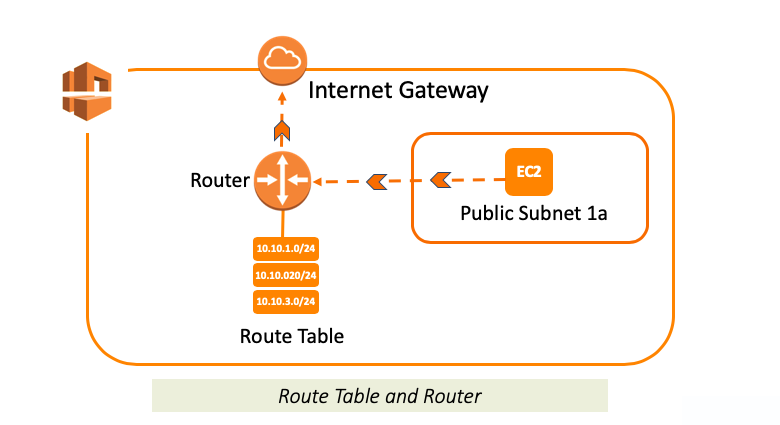
Bir Internet Ağ Geçidi, VPC'nizdeki örnekler ve internet arasındaki iletişime izin veren yatay olarak ölçeklendirilmiş, yedekli ve yüksek oranda kullanılabilir bir VPC bileşenidir.

Evimizde internete erişmemizi sağlayan ADSL veya fiber yönlendiricilerimizle internet gateawaylerini temel internet sağlayıcıları olarak düşünebiliriz.

Ayrıca, bu internet bağlantısı kendi şirket ağ altyapısı ile bu VPC arasında doğrudan bir bağlantı olarak yapılabilir. Bu sisteme VPN Ağ Geçidi de denir.

Kısacası, VPC dış dünyaya VPN Ağ Geçidi veya İnternet Ağ Geçidi olmak üzere iki temel yolla bağlanabilir.

Route Table and Router



Router Tablosu, ağ trafiğinin nereye yönlendirildiğini belirlemek için kullanılan bir dizi kuraldır. VPC altındaki tüm trafik yönlendirmelerini sağlar.

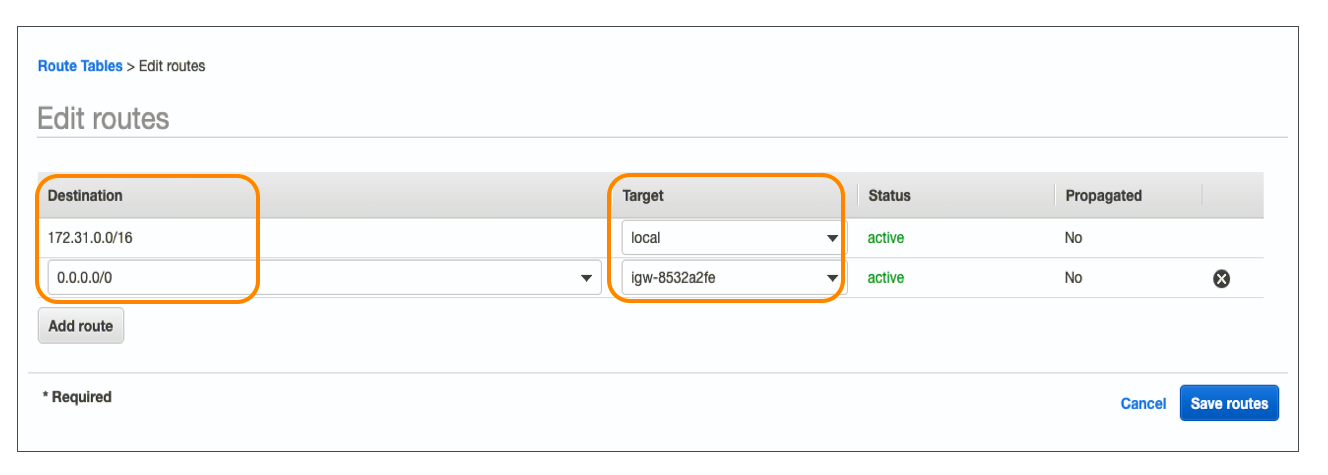
Router Tablosu, X hedefinden Y hedefine veya internete nasıl gidileceğini ve hangi yoldan kullanılacağını açıklayan kabaca yapılandırma dosyalarıdır.

Yönlendiriciler, Router Tablolarını yöneten bileşenlerdir ve ağ içinde “intersections” görevi görürler.

Her AWS VPC'de bir VPC yönlendirici bulunur.

Kısaca, Router Tablosunu bir kurallar kümesi olarak görürsek, Yönlendirici bu kuralları yürütür.

Burada, aşağıda görülen Router Tablosu örneği.



Hedef Sütun'da bir yere ulaşmak istiyorsanız, Hedef Sütun'daki değere yönlendirileceksiniz

Örneğin, bu rota tablosu sayesinde igw-8532a2fe (Internet Ağ Geçidi) kullanarak 0.0.0.0/0'a (İnternetin herhangi bir yerinden) ulaşabilirsiniz.

Network ACLs

Network ACL, Network Access Control (Ağ Erişim Kontrol) Listeleri anlamına gelir. VPC'niz için subnet içine ve dışına giden trafiği kontrol eden bir güvenlik bileşenidir. Başka bir deyişle, Subnet Network ACL’leri Subnetların güvenlik duvarıdır

Network ACL'leri subnet tabanlı güvenlik bileşenleridir.

VPC'niz otomatik olarak değiştirilebilir bir varsayılan Network ACL'si ile birlikte gelir. Varsayılan olarak, tüm gelen ve giden IPv4 trafiğine izin verir.

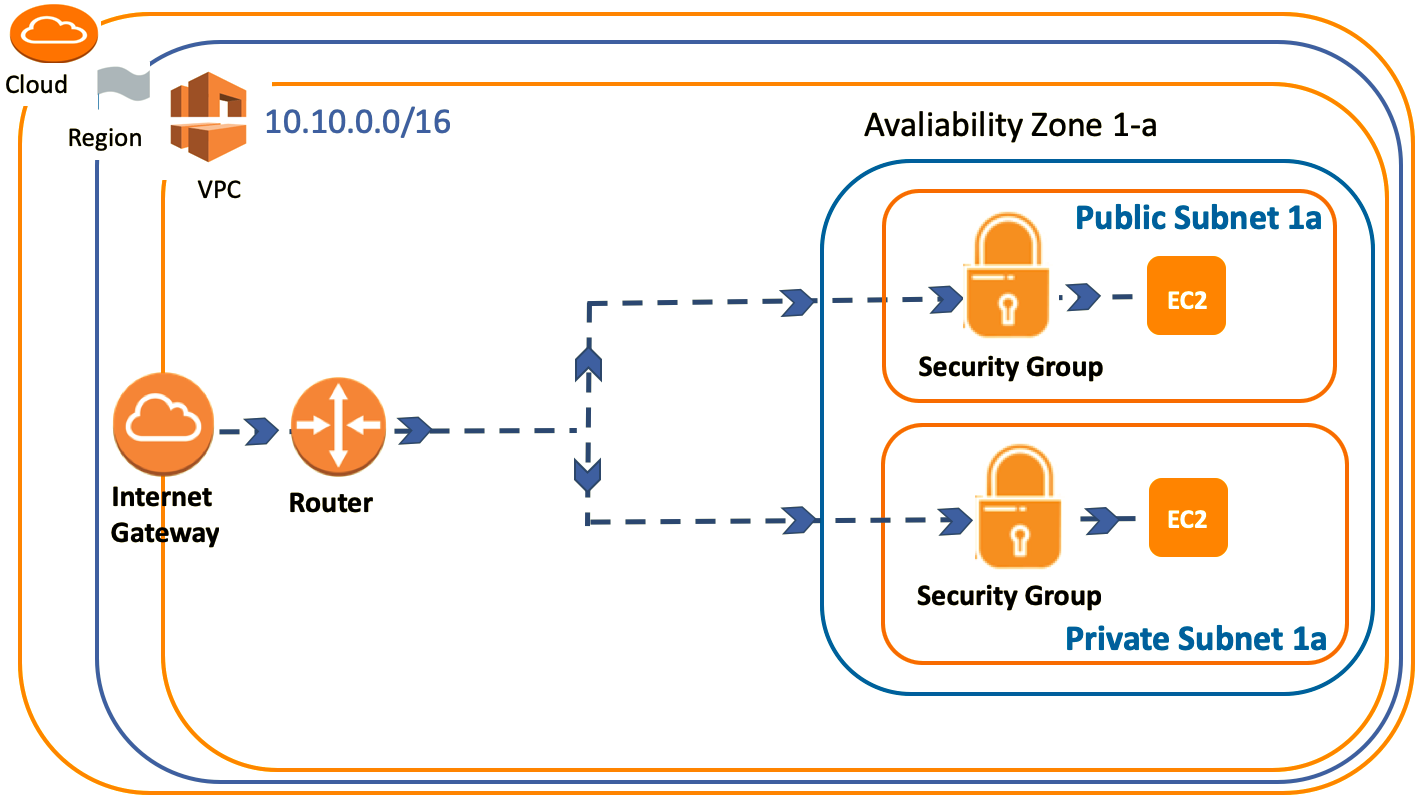
Kaçının! :

Varsayılan Network ACL sinden farklı olarak, yeni bir ağ oluşturmak istiyorsanız, kural ekleyene kadar tüm gelen ve giden trafiği reddeder

VPC'nizdeki her subnet bir Network ACL ile ilişkilendirilmelidir. Bir subnet açıkça bir Network ACL ile ilişkilendirmezseniz, subnet otomatik olarak varsayılan Network ACL 'si ile ilişkilendirilir.

Birden çok subnet Network ACL’leriyle ilişkilendirebilirsiniz. Ancak, bir subnet tek Network ACL 'si ile ilişkilendirilebilir.

Security Groups



Network ACL'lerine ek olarak, güvenlik önlemleri için VPC'de Security Groups da oluşturabiliriz.

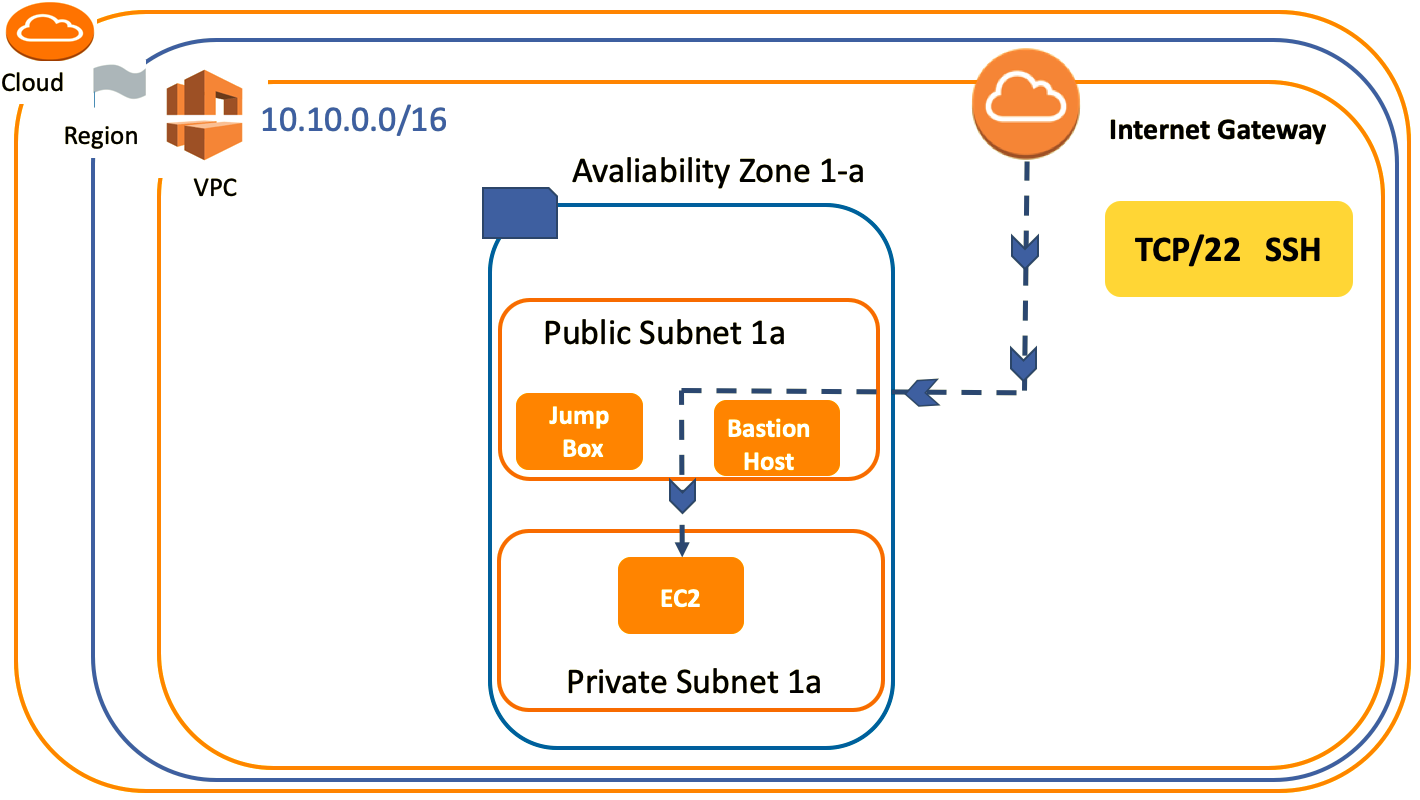
EC2 bölümünde de belirtilen Security Group, örneğe hangi trafiğin erişeceğini belirlemek için kullanılır.

Başka bir deyişle, Security Group, sanal bir Güvenlik Duvarı örneğidir.

Security Group örnek tabanlı bileşenlerken, Network ACL'leri subnet tabanlıdır. Bu nedenle, örneğin herhangi bir subnet de gelen ve giden trafik hakkında hem Security Group’larını hem de Network ACL’lerini dikkate almanız gerekir.

VPC'nizdeki bir Subnetdaki her bir örnek farklı bir Security Group atanabilir. Bir VPC'de bir örnek başlattığınızda, bir örnekle beş güvenlik grubuyla ilişkilendirebilirsiniz.

### Bastion Host/Jump Boxes



Adından da anlaşılacağı gibi, Public Subnet, Public internete kapalıdır. Ancak, bazen Public Subnet'da bulunan instance erişmemiz gerekir. Bu nedenle, bu iş için bir proxy sunucusu / instance, Bastion Host kullanıyoruz.

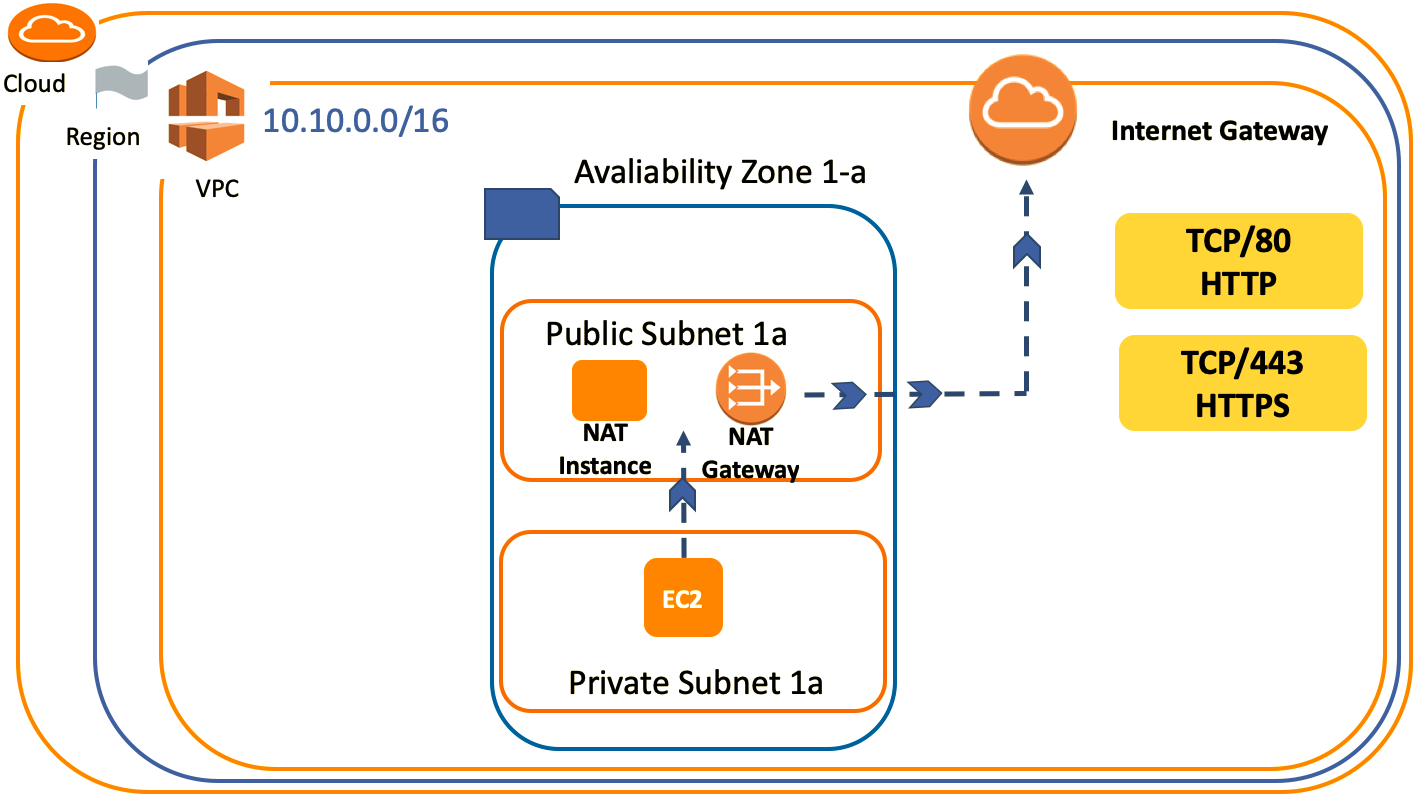
Bir Bastion Host, Internet'ten Özel bir Subneta erişim sağlamak için kullanılan bir sunucu / instance’dır.

Bastion Host, Genel Subnet’larda başlatılır ve Public Subnetdaki instance için proxy görevi görür. Altyapınıza yapılan saldırıları azaltarak güvenlik sağlar.

SSC veya RDP kullanan Jump box olarak da bilinir.

Bastion Host / Jump Box'lar, Public Subnetdaki instance’a gelen inbound trafik için kullanılır.

### VPC NAT Gateway & NAT Instance



NAT, AWS'de Ağ Adresi Çevirisi anlamına gelir. İnstance’ınız private subnette ise doğrudan İnternet'e bağlanamazsınız. Güvenlik önlemi nedeniyle, private subnetiniz giden internet bağlantısını engeller.

Ancak, bu sorunu çözmek için NAT Gateawaylerini veya public subnette 'da oluşturulan NAT Instance’ı proxy olarak kullanabiliriz.

Bu nedenle, private subnetinizdeki EC2 instance’sinden internete bağlanmak istiyorsanız, Public subnet'de NAT Gateawayleri veya NAT Instance oluşturmanız gerekir. Ardından bu bileşenler aracılığıyla EC2 Instance’nize bağlanırsınız.

Ancak, bir NAT instance’ının ve NAT Gateaway’in, private instance’ınıza gelen ağ trafiğini engellerken, giden internet bağlantısına izin vermesi önemlidir.

NAT Instance:

NAT Gateawayleri veya NAT Instance’ı hemen hemen benzer şeylerdir ve aynı işlevselliği sağlarlar, ancak NAT Gateaway AWS tarafından yönetilen bir NAT hizmetidir, ancak NAT Instance’ı müşteri tarafından belirlenir ve yönetilir. Aslında, NAT Gateawayleri yaygın olarak kullanılmaktadır NAT instance’lardan daha gerçek zamanlı olarak ve NAT Gateawayleri ile multiple AZ ye erişilebilir.

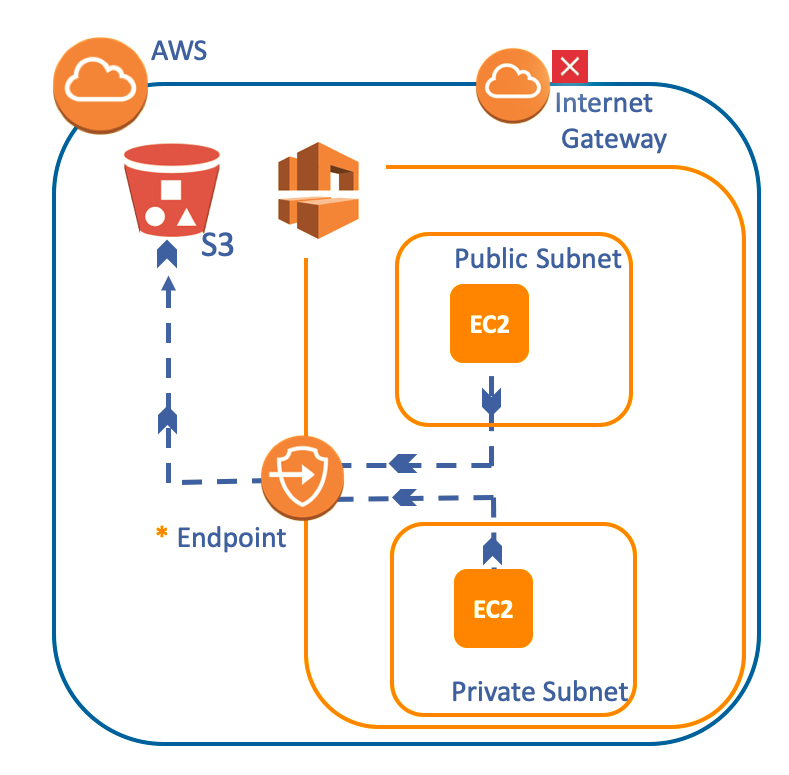
Avoid

NAT Gatewayni Bastion ana bilgisayarı olarak kullanamazsınız. Özel bir alt ağdaki bir instance’a SSH veya RDP ile bağlanırsanız, Bastion Host'u yapılandırmanız gerekir. NAT Gatewayni kullanamazsınız.

Tips

Bastion Host / Jump Boxes Inbound trafik için kullanılırken, NAT Gateway / NAT Instance Outbound trafik için kullanılır.

VPC Endpoint



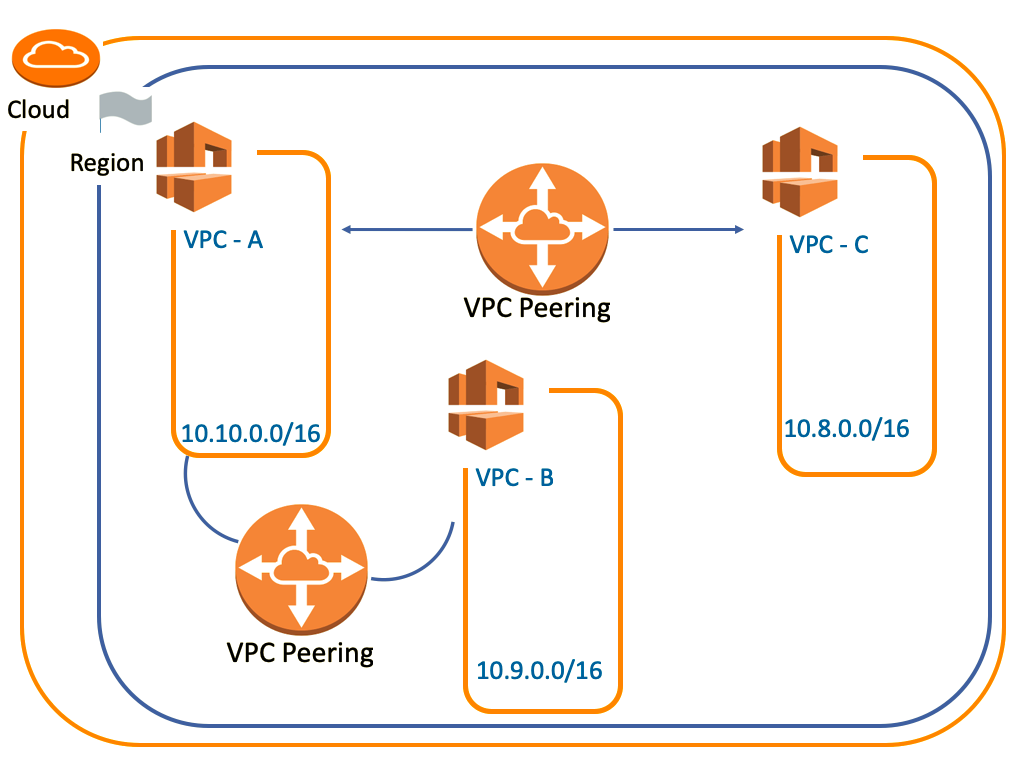
VPC Endpoint, VPC'nizi S3 gibi desteklenen AWS servislerine özel olarak bağlamanızı sağlayan bir bileşendir.

Aslında, VPC'niz ve diğer server arasındaki trafik Amazon ağından ayrılmaz. Bu sanal ortamda, AWS bize böyle bir kısayol sunuyor.

VPC Endpoint yatay olarak ölçeklendirilmiş, yedekli ve yüksek oranda kullanılabilir bir VPC bileşenidir. Böylece ağ trafiğinizde kullanılabilirlik riskleri veya bant genişliği kısıtlamaları uygulamadan VPC'nizdeki instance’lar ve serverlar arasında iletişime izin verir.

VPC Endpoint sayesinde, VPC'nizdeki Instance’lar, server’daki kaynaklarla iletişim kurmak için genel adresler gerektirmez. Çünkü, Internet Gateway, VPN Bağlantısı vb. Gerektirmeden PrivateLink tarafından desteklenen VPC Endpoint hizmetleri.

VPC Peering



Bir VPC peering, iki VPC arasındaki bir ağ bağlantısıdır.

Özel IPv4 adreslerini veya IPv6 adreslerini kullanarak aralarındaki trafiği yönlendirmenize olanak tanır. Farklı VPC'deki instance’lar aynı ağdaymış gibi birbirleriyle iletişim kurabilir.

İki VPC arasında gözetleme onlara özgüdür. Bunun ne anlama geldiğini anlamak için yukarıda görülen resmi değerlendirelim.

VPC-A ve VPC-B arasında zaten VPC Peering'iniz olduğunu varsayalım. VPC-A ve VPC-C arasında yeni VPC eşlemesi oluşturursanız, VPC-B ve VPC-C arasındaki bağlantı otomatik olarak gerçekleşmez. Bağlantıları için VPC-B ve VPC-C arasında başka bir VPC peering oluşturmanız gerekir.

Elastic IP

Elastic IP adresi, dinamik bulut bilgi işlem için tasarlanmış bir Statik IPv4 Adresidir. Kısacası, Elastik IP örneğiniz için kalıcı bir IP'dir.

Public IP adresleri dinamiktir. Örneğinizi durdurur / başlatırsanız, yeni bir genel IP atarsınız. Ancak, Elastic IP'ler hesabınıza tahsis edilir ve aynı kalır.

Elastik IP'ler dinamik olarak yeniden eşlenebilen IP adresleridir, bu yüzden bunları başka bir instance’a eklemek ya da eklememek size bağlıdır.

Ama neden Elastik IP'ye ihtiyacımız var?

Elastik IP'leri, özellikle avantajları veya kullanımının zorunlu olduğu durumlar nedeniyle çeşitli nedenlerle kullanıyoruz

Örneğin;

Elastik IP adresine bir lisans atamayı tercih edebiliriz,

Bazı uygulamaların statik IP kullanması yasal bir gereklilik olabilir.

NAT Gateway ve Route 53 gibi bazı AWS bileşenleri, oluşturma, çalıştırma veya kurulum işlemi sırasında Elastik IP'ye ihtiyaç duyabilir.

Ama şimdilik, bizi ilgilendiren kısım NAT Gateway olacak ve bunu sonraki derslerde ayrıntılı olarak göreceğiz.

Avoid:

Elastik IP'ler bir instance tarafından kullanıldığı sürece tamamen ücretsizdir. Ancak, Amazon, ayırdığınız ve kullanmadığınız her EIP için 0,01 $ / saat ücret alır. Kısa vadede artık kullanmayacaksanız, Elastik IP'yi veya NAT Gateway gibi ilişkili bir bileşeni sonlandırmayı unutmayın.